EX PARTE OR LATE FILED

gpm associates

306 Chuniloti Circle
Loudon, TN 37774-2607
(615) 458-4519
(207) 778-3647 (6/1 - 9/20/94)

DOCKET FILE COPY ORIGINAL

April 21, 1994

RECEIVED
APR 25 1994
MAIL BRANCH

Mr. William P Caton, Acting Secretary
Office of the Secretary
Federal Communications Commission
Washington, D.C. 20554

Re: CC Docket 93-292

Dear Mr. Caton:

We are submitting this Ex Parte presentation in response to your request for comments on the Notice of Proposed Rulemaking issued December 2, 1993. We specifically address ways to prevent toll fraud.

Our patent titled "Transaction Authentication Using a Centrally Generated Transaction Identifier" was allowed March 8, 1994. The GPM process is particularly appropriate for preventing completion of fraudulent calls originating in pay phones, phones used to remotely access PBX systems and cellular or other wireless phones[1].

It is like other authentication methods that change authentication codes frequently. However, the GPM process changes codes unpredictably for each transaction and it is designed to make compromise by anyone impractical, including its designers and those employing the system. Possession of equipment containing GPM microprocessors is no threat, nor is knowledge of the algorithms. Hacking is effectively prevented as are attempts to derive sensitive data by applying large amounts of computer power to transaction information that might be collected by electronic surveillance.

The overall process is described in Appendix A, the first four pages of our patent application. Appendix B describes how we would apply our process to cellular and other wireless phone systems[2]. Its application to remote access of PBX networks and phone credit cards is shown in Appendix C and Appendix D, respectively.

No. of Copies rec'd 0+4
List ABCDE

[1]The GPM process also is effective for authenticating transactions for interactive television and electronic funds transfer systems and for preventing unauthorized access to computer networks.

[2]Implementation of the GPM process for cellular phones now in the field would require changes or retrofitting which the carriers are very reluctant to do because of costs and customer impact. One way to avoid all that is to implement GPM on a going forward basis, perhaps as the change from analog to digital cellular systems is made. If that is too slow, our patent provides for use of an access module that could be provided current phone users as a means to effect the changeover without recalling or exchanging phones. The access module would be like that described for remote access to PBX systems in Appendix C.

We note AT&T's views that any solutions should avoid changes to their network that would decrease call completion rates and that all reasonable fraud prevention methods should be considered and implemented before any new rules assign liability for charges. Also, SPRINT and the Commission seem to agree that liability for fraudulent charges should be assigned to those in the best position to prevent them from being incurred.

The GPM process would require changes to carrier networks. It would cause some delay in call completion rates as would implementation of any authentication process. It seems that authentication procedures in use now or being considered also impose delay and that they perhaps are not as effective in preventing toll fraud as our process. The GPM process would cause less delay because, unlike other systems, it compares codes without need for inversion or decryption. This simplifies equipment needs and the process significantly. Furthermore, GPM uses existing call setup data to develop authentication codes. For those calling situations that do not now require PIN, it would be the only additional data item to be input[3].

AT&T's second suggestion about implementing reasonable preventive means before assigning liability for fraudulent charges could be satisfied, we believe, by our process. That would seem to tie in with the view of SPRINT and the Commission that liability should be assigned to those in the best position to prevent fraud and who fail to do so. It may even be that the pressure to assign liability would disappear if toll fraud charges were to be reduced significantly.

CONCLUSION

GPM Associates requests Commission consideration of its process for preventing toll fraud. We know of no other system as potentially capable of preventing unauthorized calls.

Respectfully submitted,

Robert A. Montgomery
GPM Associates

cc: Honorable Alfred C. Sikes, Commissioner, FCC
Honorable Ervin S. Duggan, Commissioner, FCC
Honorable Andrew C. Barrett, Commissioner, FCC
Honorable Sherie P. Marshall, Commissioner, FCC
Honorable James H. Quello, Commissioner, FCC
Honorable Edward J. Markey, Chairman, Subcommittee of Telecommunications and Finance, U.S. House of Representatives
Linda Dubroof, Senior Attorney, Common Carrier Bureau, FCC
Kurt Schroeder, Common Carrier Bureau, FCC

---

[3]As shown in the appendices hereto, a variety of techniques would be employed to protect PIN from physical observation and other detection efforts according to the circumstances involved.

GPM Associates' Ex Parte Presentation: CC 93-292, Toll Fraud
General Description of the GPM Process

Filing Date: 9/28/93

TITLE: **Transaction Authentication Using a Centrally Generated Transaction Identifier**

Inventors: Milton Goldfine, Loudon, TN
Marvin Perlman, Granada Hills, CA
Robert A. Montgomery, Loudon, TN

BACKGROUND OF THE INVENTION

1. Field of Invention:

This invention authenticates a transaction request in order to permit progress of a transaction based on a match between an authentication code generated by the requestor of the transaction and an authentication code generated by an authentication agency.

2. Brief Description of the Prior Art:

Central authentication of remote transactions is an important mode of business conduct. Remote access to electronic funds transfer networks must be authenticated to prevent theft of funds. Access to communications systems, such as cellular mobile radio systems, must be authenticated to prevent theft of communication services. Authentication is also important in governing electronic access to computer networks and interactive television and physical access to secured locations. Operators of these kinds of systems have developed a number of different techniques for reducing the susceptibility of their systems to various forms of fraud. However, almost all of these techniques can be circumvented by sophisticated misusers with enough computer resources at their disposal or by dishonest employees who can access the systems at various exposed points to steal access code information.

Many of the authentication techniques use combinations of passwords and personal identification numbers (PINs) to attempt to verify that the user attempting to access a network or service

is authorized for access. Unauthorized access using PINs and passwords improperly obtained can be somewhat reduced by requiring users to periodically change these codes. A personal identification system disclosed in U.S. Pat. #4, 376, 279 uses a PIN secretly selected by the user, a code number secretly selected by officers of the authenticating agency and an irreversible transform secretly selected by the manufacturer of the system to produce a code number that is magnetically encoded onto a user card, such as a credit card or banking access card. Since only the user knows the selected PIN, the user's entry of that PIN, after inserting the card into the system presumably establishes that authority of that user to access the system. However, even though the system is partitioned to protect different portions of the access code information, changing access codes is cumbersome, so that the same information is used over and over again. An eavesdropper or other person that can obtain access to the transaction data and with enough computer power may, over time, accumulate enough information to learn the access code and gain unauthorized entry.

Theft of telecommunication services through eavesdropping on cellular mobile radio calls has become a major problem. The eavesdropper captures or derives the caller's access code, builds it into his radio unit, and makes subsequent unauthorized calls billed to the original caller. A long period of time could go by before this misuse is discovered and the access code changed. Hackers seeking access to telecommunication and computer networks program their computers to try thousands of access codes in an attempt to find one that works. Once a successful code is found, the hacker can gain network access. Similar problems will exist for emerging interactive television services, such as entertainment and home shopping. Authentication techniques that use repeatedly transmitted access codes are susceptible to various sophisticated attacks. Some technique is needed to keep the attackers off balance.

GPM Associates' Ex Parte Presentation: CC 93-292, Toll Fraud
General Description of the GPM Process

SUMMARY OF THE INVENTION

The transaction authentication method that is the subject of the present invention uses a centrally generated identifier that is specific to each transaction request to assure that the access information being transmitted from point to point in the system is different for each transaction attempt. In this transaction authorization process and apparatus, each access attempt transmitted to an authentication agency causes the agency to produce a request identifier unique to that request. The request identifier is transmitted back to the authentication code generator of the user initiating the access attempt, and to an authentication code generator in the agency. The agency also retrieves a user identifier from a database and sends it to its authentication code generator. Both the user's authentication code generator and the agency's authentication code generator independently combine, through identical or complementary transformations, the user identifier and the request identifier to form a user authentication code and an agency authentication code. The two authentication codes are presented to a comparator, which issues a permit signal only if the comparison indicates a match between the two authentication codes. The permit signal is transmitted to a transaction control device to permit the transaction to proceed. Since the authentication code is unique to each transaction attempt, interception of an authentication code will not permit an unauthorized user to successfully initiate another transaction. As an additional security feature, the use of an irreversible transformation in the authentication code generator would prevent decoding of an intercepted authentication code and would not allow an unauthorized user to derive the user identifier associated with the transaction. As required by the particular application, additional levels of security can be achieved by using encryption steps (reversible) in combination with the irreversible transformations at selected points in the process.

GPM Associates' Ex Parte Presentation: CC 93-292, Toll Fraud
General Description of the GPM Process

This invention produces a flexible transaction authentication architecture that can be used to meet the security needs of a diversity of transactions, such as authorizing a call to a remote access port of a telecommunication network or a cellular mobile radio call to access the network, allowing remote access to a computer network, identifying a user as an authorized electronic funds transfer agent or legitimate user of interactive television services, and permitting physical access to a secured location. Each of these transactions has different points of vulnerability to eavesdropping from the outside or compromise by dishonest insiders. The inventive architecture permits use of transformation and/or encryption of the authentication information at different points in the system dependent on an analysis of the particular application's vulnerabilities. In any event, the authentication information will be different for each transaction attempt, greatly impeding or entirely foiling efforts to successfully complete an unauthorized transaction.

With modern integrated circuit technology, the transformation involved can be economically realized in a microprocessor or special purpose VLSI chip. This architecture gives the authorized user an economic advantage over the intended intruder. Since the authentication code changes in a virtually unpredictable way, an eavesdropper or intruder, collecting large amounts of data and applying much computer power, would find it practically impossible to determine a usable authentication code. However, the subject system compares authentication codes in their transformed or encrypted state without requiring inversion or decryption, which greatly simplifies the required equipment. The organization and operation of the invention can be better understood from consideration of the following detailed description of illustrative embodiments when read together with the accompanying drawings.

Appendix B

GPM Associates' Ex Parte Presentation: CC93-292, Toll Fraud
Application of the GPM Process to Cellular Phone Systems

Discussion of Figure 1, Cellular System Black Box Diagram:

This diagram shows the GPM process in the form of three blocks to help explain the process in a simple form. The blocks represent;
(1) Calling Cellular Phone
(2) Central Office
(3) Receiving Phone.

The Calling Cellular Phone has three inputs; viz., PIN, Request ID (RID), and Communication Data. Its outputs are Transaction Request, Authentication Code and Communication Data.

The Central Office (C.O.) receives the three Calling Cellular Phone outputs and transmits RID to the Calling Cellular Phone and Communication Data to both phones. For the GPM process, the principal C.O. function is to permit only properly authenticated cellular calls.

The operational flow depicted by figure 1 is as follows:
(1) PIN is entered to Calling Cellular Phone either by Keypad or by an Enabling Key containing PIN.
(2) An 'off-hook' or 'transmitter on' signal is a Transaction Request.
(3) In response to the Transaction Request, the C.O. transmits a Request ID that is unique to each request.
(4) At the calling phone, PIN and other data not depicted plus RID are transformed into an Authentication Code that is transmitted to the C.O.
(5) At the C.O., information (not shown) is retrieved from a data base and transformed[1] along with RID into a C.O. authentication code for the particular transaction request in process.
(6) Authentication codes produced by the calling phone and the C.O. are compared at the C.O. and the call request allowed only if the two codes are identical.
Notes: (a) PIN is not stored or transmitted.
(b) Authentication Codes change unpredictably for each call because RID is transaction specific.

Figure 2 lists the Cellular Phone System Black Box requirements and is self-explanatory.

---

[1]The transformation may use encryption or irreversible transformation. Irreversible transforms, as used in the GPM process, are such that the cost of resources required to determine PIN greatly exceed the potential reward.

GPM Associates' Ex Parte Presentation: CC93-292, Toll Fraud
Application of the GPM Process to Cellular Phone Systems

Figure 3 depicts the flow of the GPM process for cellular phone applications.

Definitions of new terms:
Enabling Key: a removable key that contains PIN.

Transformer: an electronic entity to encrypt or irreversibly transform data.

User ID Code: the encrypted or transformed Electronic Serial Number (ESN) of the Calling Cellular Phone and PIN.

Transaction Request (TR): a Calling Cellular Phone request for dial tone from its serving central office.

Request ID (RID): a number that changes unpredictably for each transaction (call) request. It may be a function of time and date or a random number generator.

Transaction Controller: an electronic switch for completing or disallowing a communication connection.

Operational Sequence at the Calling Cellular Phone:
PIN is entered by Keypad or Enabling Key[2].

The request for 'dial tone' is the Transaction Request causing the C.O. to generate a unique Request ID and transmit it to the calling phone.

PIN and ESN are entered into Transformer # 1 and encrypted or irreversibly transformed into a User ID Code.

The RID received from the C.O. and the User ID Code enter Transformer # 2 to be encrypted or irreversibly transformed into Authentication Code 1 (AC 1).

AC 1 is transmitted to the C.O.
(See Operational Sequence at the Central Office, next page.)
'Dial tone' is received if the authentication codes produced by the calling phone and C.O. match. Then the caller proceeds to make the call as usual.

[2]The Enabling Key provides security in that it is needed to operate its corresponding phone. Users should keep their Enabling Keys separate from their phones except when communicating.

GPM Associates' Ex Parte Presentation: CC93-292, Toll Fraud
Application of the GPM Process to Cellular Phone Systems

Operational Sequence at the Central Office:

Request ID is generated and transmitted to the calling phone based on an 'off hook' or 'transmitter on' signal. It also is routed to Transformer # 3 in the C.O.

ESN of the Calling Cellular Phone is routed to the User ID Code Database.

User ID Code (identical to the output of Transformer #1) is retrieved from the database based on ESN and sent to Transformer # 3.

Transformer # 3 encrypts or irreversibly transforms RID and User ID Code into Authentication Code 2 (AC 2).

Authentication Codes 1 & 2 are sent to the Comparator which issues a permit signal to the Transaction Controller if they match.

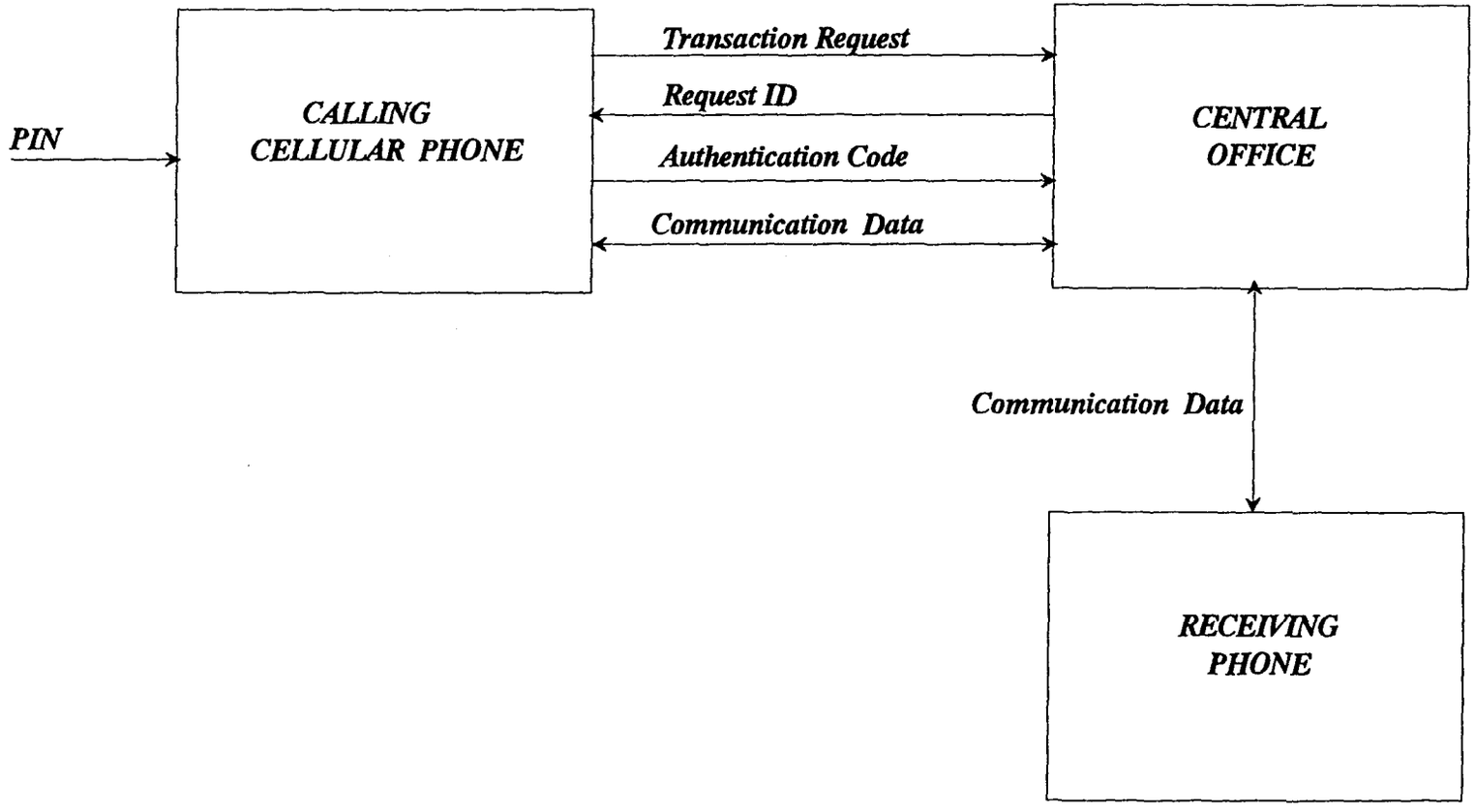
Based on a permit signal, the Transaction Controller issues 'dial tone' to the calling phone and handles the call as usual.

GPM Associates' Ex Parte Presentation: CC 93-292, Toll Fraud
Application of the GPM Process to Cellular Phone Systems

gpm associates

GPM TRANSACTION AUTHENTICATION PROCESS

CELLULAR PHONE SYSTEM BLACK-BOX DIAGRAM



3/29/94

FIGURE 1

gpm associates

GPM TRANSACTION AUTHENTICATION PROCESS

CELLULAR PHONE SYSTEM
BLACK-BOX REQUIREMENTS

o *CALLING CELLULAR PHONE*
- *Generate a **Transaction Request***
- *Accept the **PIN** and the **Request ID***
- *Generate the **Authentication Code** from **PIN, Request ID,** and other numbers*
- *Send **Communication Data** to the **CENTRAL OFFICE***

o *CENTRAL OFFICE*

- *Receive **Transaction Request***
- *Generate a **Request ID** in response to the **Transaction Request***
- *Send the **Request ID** to the CALLING CELLULAR PHONE*
- *Receive the **Authentication Code** from the CALLING CELLULAR PHONE*
- *Generate its own **Authentication Code** from **Request ID** and stored data*
- *Compare the two **Authentication Codes***
- *Allow **Communication Data** to flow between the CALLING CELLULAR PHONE and the **RECEIVING PHONE** only if the **Authentication Codes** match*

3/29/94

FIGURE 2

GPM Associates' Ex Parte Presentation: CC 93-292, Toll Fraud
Application of the GPM Process to Cellular Phone Systems

GPM TRANSACTION AUTHENTICATION PROCESS

CELLULAR PHONE APPLICATION

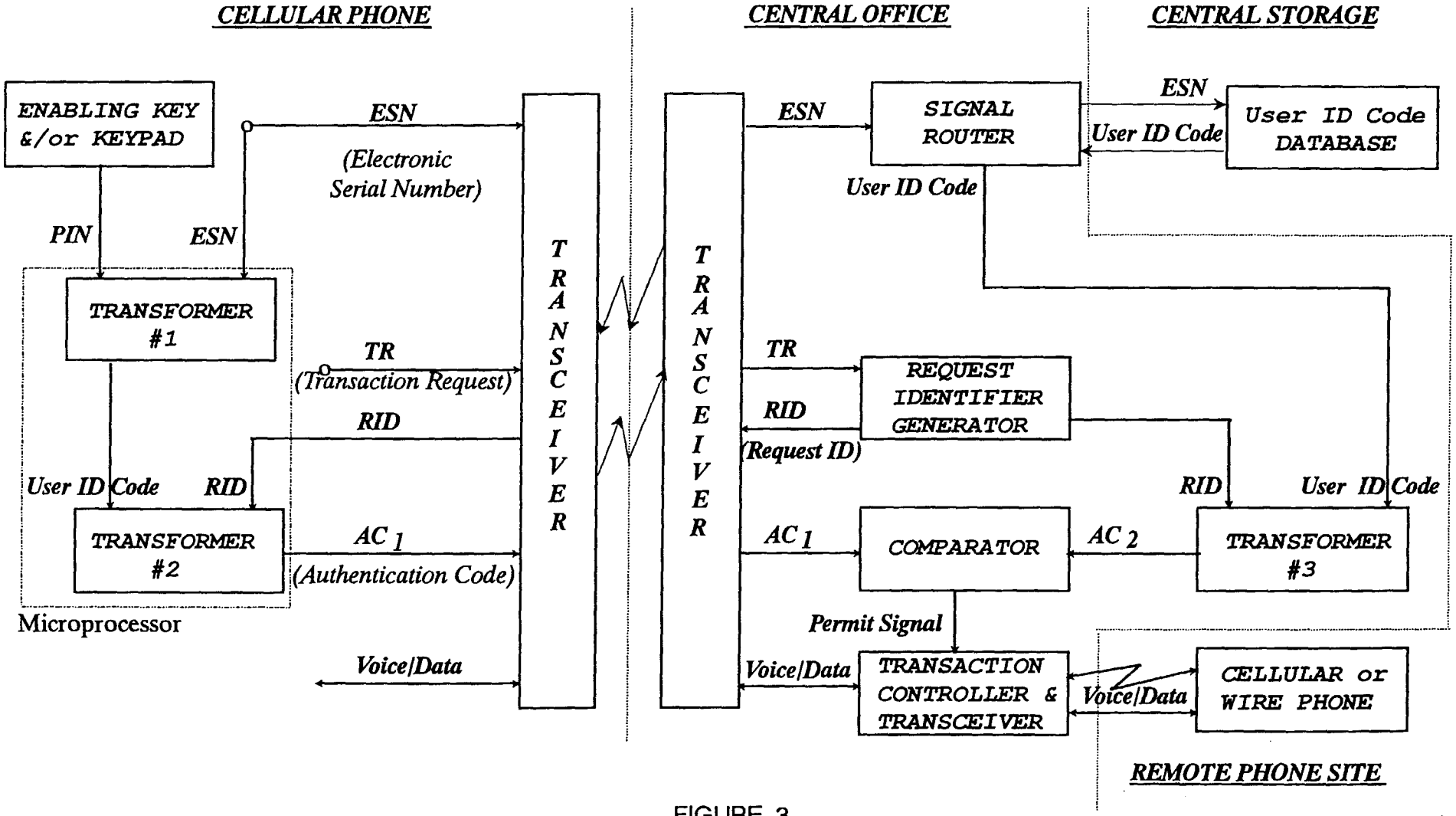


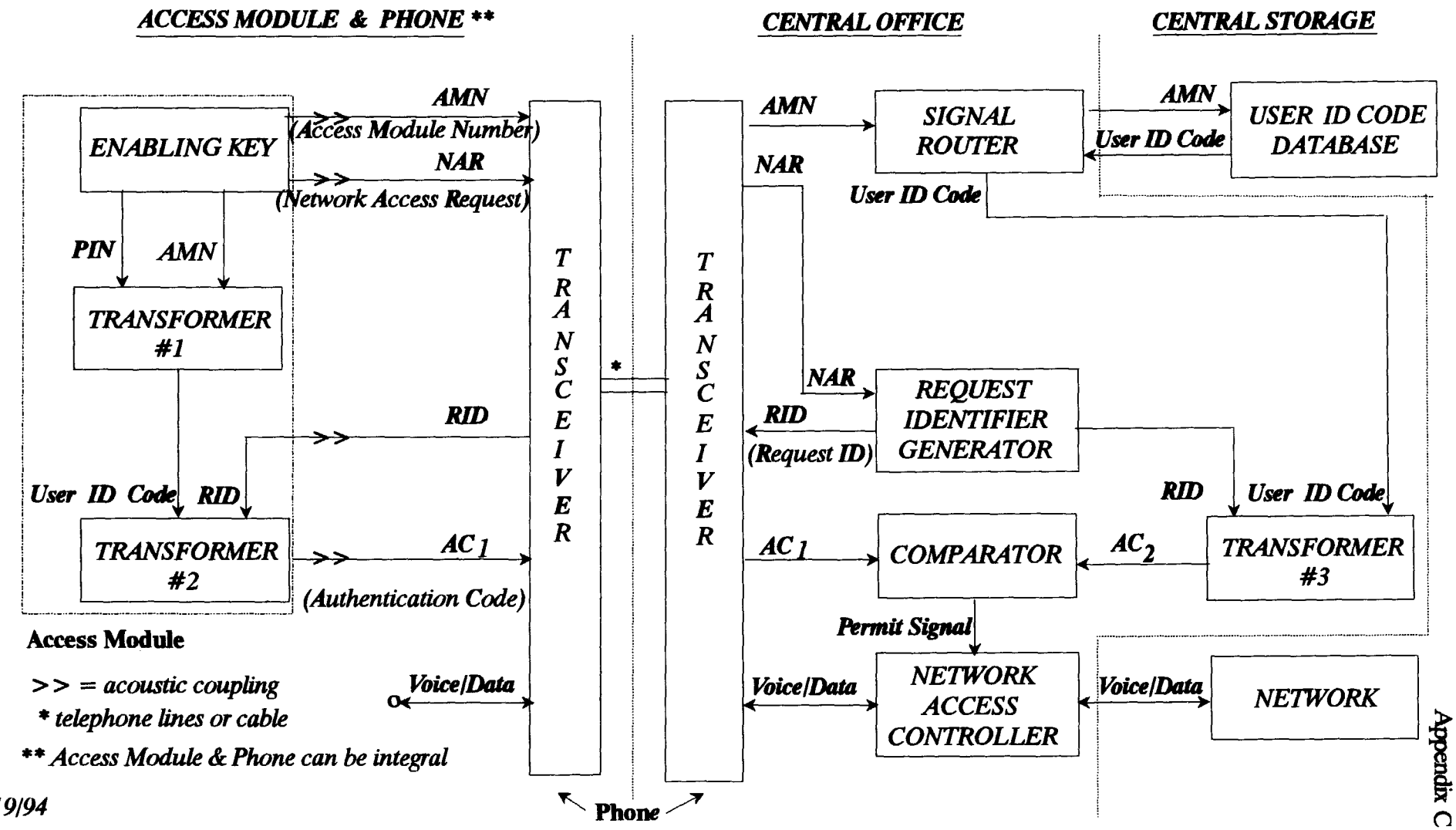
FIGURE 3

3/29/94

Appendix B

GPM TRANSACTION AUTHENTICATION PROCESS

PBX NETWORK ACCESS APPLICATION

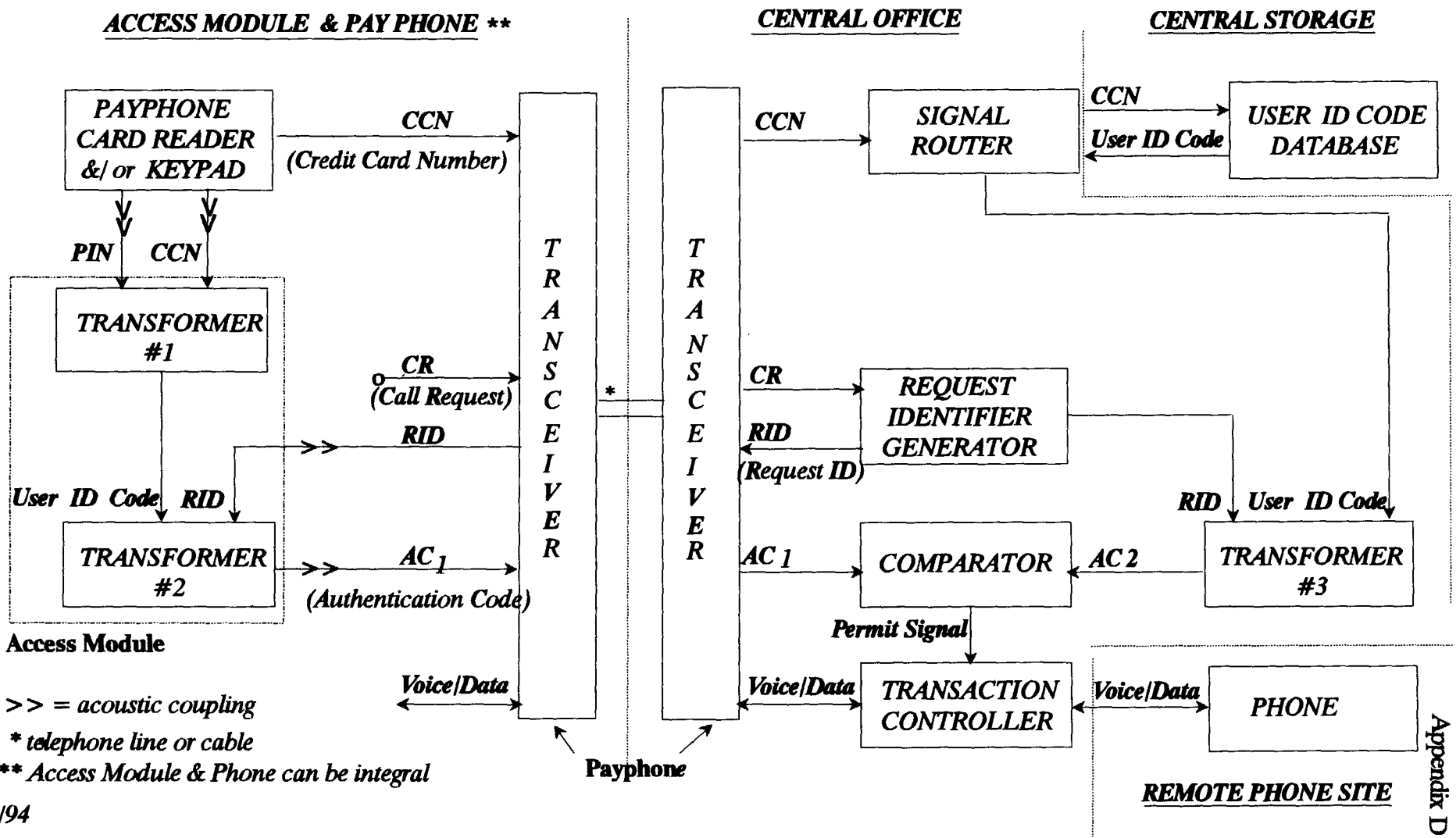


4/19/94

Appendix C

GPM TRANSACTION AUTHENTICATION PROCESS

PAY PHONE CREDIT CARD APPLICATION



Appendix D